**Part 1:**

**Q.1:**

Graphical user interface, text

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text

Description automatically generated

**Q.2:**

I think that a good purpose of hiding a simple yet sensitive message content in a spam format is that spam is so common that many people, including myself, don’t think twice about seeing a spam email and deleting it. If you wanted to sift through real spam emails looking for a hidden spam message, I think that it would be difficult to detect a hidden message, unless you knew that was what you were looking for. This adds a easy and simple step to hiding a message that could be easily overlooked, providing a base level of security. This allows a user to send an encrypted message without it looking like an encrypted message!

**Part 2:**

**Q.3:**

**Graphical user interface, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**Q.4:**

**Issuer:**

GeoTrust Global TLS RSA4096 SHA256 2022 CA1

DigiCert, Inc.

**Public Key:**

Modulus (2048 bitsublic Exponent (17 bits): 01 00 01

**Signature Algorithm:**

PKCS #1 SHA-256 With RSA Encryption

**Valid until date:**

Wednesday, June 7, 2023 at 6:59:59 PM

**Thumbprint/Fingerprint:**

**SHA-256 Fingerprint:** 59 83 4C F2 56 63 CB 68 B6 9C 76 67 25 34 44 2A 6F BD 5F E8 DC AA B5 1F 1B A9 40 15 05 9E F7 BD

**SHA-1 Fingerprint:** 70 0F 54 A2 BE 4B F1 EC C1 A6 88 98 B9 37 C9 F2 29 82 56 B4

**Q.5:**

Graphical user interface

Description automatically generated

**Similarities:**

Issuer is the same.

Public key algorithm is the same.

Signature algorithm is the same.

Valid until date is the same.

**Differences:**

The public key itself is not displayed in this report.

The fingerprint values are not displayed in this report.

**Q.6:**

I think that my biggest takeaway from this Practical Exercise is that I never really gave a second thought to spam emails and that in reality the sheer amount of spam that is being sent out gives a great environment to hide an encrypted message without directly labeling it as an encrypted message. A hacker may be looking at the email traffic and might ignore spam emails allowing an encoded spam message to deliver without triggering any red flags that something encrypted is being sent/received. Another takeaway for me, is that there is a lot of information that you can collect from an SSL certificate just by looking at it which could provide valuable information. PGP is also an interesting encryption program that uses the Public Key and Private Key to increase the level of security during an email communication that needs an extra level of encryption. By using a password with this encryption, it would keep the message safe unless the third-party was also able to obtain the password for the decryption.